V Semester 23CC5O01	CYBER SECURITY AND RISK MANAGEMENT	L	T	P	C
		3	0	0	3

Course Objectives

This course aims to:

- Understand threats in networks and key security concepts.
- Explore authentication techniques and email security protocols.
- Recognize firewall functions and cybercrime investigation procedures.
- Introduce forensic tools and best practices in cyber incident response.

Course Outcomes

By the end of the course, the student will be able to:

CO No.	Course Outcome
CO1	Identify and differentiate among various cyber threats, vulnerabilities, and attacks.
CO2	Understand ethical and legal considerations in cyber security, including cyber laws and privacy concerns.
CO3	Perform basic penetration testing and assess common web application vulnerabilities.
CO4	Apply forensic investigation techniques for memory, OS, email, and network analysis using common forensic tools.
CO5	Evaluate risks and implement security policies for proactive cyber defense and incident response.

UNIT-I

Introduction to Information Security Fundamentals and Best Practices: Protecting Your Computer and its Contents, Securing Computer Networks--Basics of Networking, Compromised Computers, Secure Communications and Information Security Best Practices, Privacy Guidelines, Safe Internet Usage.

UNIT-II

Ethics in Cyber Security & Cyber Law: Privacy, Intellectual Property, Professional Ethics, Freedom of Speech, Fair User and Ethical Hacking, Trademarks, Internet Fraud, Electronic Evidence, Cybercrimes.

UNIT-III

Penetration Testing: Overview of the web from a penetration testers perspective, Exploring the various servers and clients, Discussion of the various web architectures, Discussion of the different types of vulnerabilities, defining a web application test scope and process, Defining types of penetration testing.

UNIT-IV

Web Application Security: Common Issues in Web Apps, what is XSS, SQL injection, CSRF, Password Vulnerabilities, SSL, CAPTCHA, Session Hijacking, Local and Remote File Inclusion, Audit Trails, Web Server Issues.

Forensics & Network Assurance: Forensic Technologies, Digital Evidence Collection, Evidentiary Reporting, Layered Defense, Surveillance and Reconnaissance, Outsider Threat Protection.

UNIT-V

Information Risk Management: Asset Evaluation and Business Impact Analysis, Risk Identification, Risk Quantification, Risk Response Development and Control, Security Policy, Compliance, and Business Continuity. Forensic investigation using Access Data FTK, En-Case.

Cyber Incident Analysis and Response: Incident Preparation, Incident Detection and Analysis, Containment, Eradication, and Recovery. Proactive and Post-Incident Cyber Services, CIA triangle.

Text Books

1. Anas Zakir, Cyber Security & Digital Forensics, Clever Fox Publishing, 2022.
2. Abhinav Ojha, Beginner's Guide to Ethical Hacking and Cyber Security, Khanna Publishers, 1st Edition, 2023.

Reference Books

1. Dave Kleiman, The Official CHFI Study Guide for Computer Hacking Forensic Investigator, EC-Council Press.
2. James M. Stewart, CISSP Study Guide, 6th Edition, Sybex/Wiley.

Web Resources

1. NIST Cybersecurity Framework – https://www.nist.gov/cyberframework
2. OWASP Top 10 Vulnerabilities – https://owasp.org/www-project-top-ten/
3. MITRE ATT&CK Framework – https://attack.mitre.org
4. CISA Cybersecurity Training Resources – https://www.cisa.gov/free-cybersecurity-training-resources
5. FTK Imager Download – https://accessdata.com/product-download/ftk-imager-version-4-2